Actualizar el VMware Identity Manager Conector

VMware Identity Manager 2.8
VMware Identity Manager 2.9.1

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

https://docs.vmware.com/es/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Actualización de VMware Identity Manager Connector 5

1 Acerca de actualizar el conector de VMware Identity Manager 7

2 Preparar la actualización de VMware Identity Manager Connector 9
- Requisitos para la actualización 9
- Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager Connector 10
- Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager Connector 10

3 Realizar una actualización en línea de VMware Identity Manager Connector 13

4 Realizar una actualización de VMware Identity Manager Connector sin conexión. 15
- Preparar un servidor web local para la actualización sin conexión 15
- Configurar el conector y realizar una actualización sin conexión 16

5 Realizar la configuración después de actualizar el conector 17

6 Resolver problemas de actualización 19
- Consultar los registros de errores de la actualización 19
- Restaurar snapshots del conector 19
- Recopilar un paquete de archivos de registro 20

Índice 21

Actualización de VMware Identity Manager Connector

En el documento *Actualizar el conector de VMware Identity Manager* se describe cómo actualizar su instancia de VMware Identity Manager Connector. Si prefiere hacer una instalación nueva, consulte *Instalar y configurar VMware Identity Manager Connector*. Recuerde que en una nueva instalación no se conservan las configuraciones existentes.

Son compatibles las siguientes rutas de actualización:

- De las versiones 2.3 , 2.4, 2015.10.1 o posteriores a la última versión disponible

Para obtener más información sobre cómo utilizar la instancia actualizada del conector, consulte la guía del administrador de *VMware Identity Manager*.

Público objetivo

Esta información está dirigida a todos los que instalen, actualicen y configuren VMware Identity Manager Connector. La información está escrita para administradores de sistemas Windows o Linux con experiencia y que estén familiarizados con la tecnología de máquinas virtuales.

Acerca de actualizar el conector de VMware Identity Manager 1

Puede actualizar VMware Identity Manager Connector en línea o sin conexión.

De forma predeterminada, el conector utiliza el sitio web de VMware para el procedimiento de actualización y, para ello, es necesario que el dispositivo del conector tenga conexión a Internet. También se debe configurar el servidor proxy para el dispositivo del conector, si corresponde.

Si la instancia del conector no dispone de conexión a Internet, se puede realizar la actualización sin conexión. Para realizar una actualización sin conexión, se debe descargar el paquete de actualización y configurar un servidor web local para alojar el archivo de actualización.

Son compatibles las siguientes rutas de actualización:

- De las versiones 2.3 , 2.4, 2015.10.1 o posteriores a la última versión disponible

Preparar la actualización de VMware Identity Manager Connector 2

Para preparar la actualización del conector, antes debe realizar un número de tareas requeridas, como buscar las actualizaciones disponibles y configurar las opciones del servidor proxy del dispositivo, si corresponde.

Este capítulo cubre los siguientes temas:

- "Requisitos para la actualización," página 9
- "Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager Connector," página 10
- "Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager Connector," página 10

Requisitos para la actualización

Antes de actualizar el conector, realice estas tareas.

Requisitos previos para la actualización online

- Verifique que el dispositivo conector pueda resolver y acceder a la dirección vapp-updates.vmware.com en el puerto 80 mediante HTTP.
- Confirme que existe una actualización del conector. Ejecute el comando correspondiente para comprobar si hay actualizaciones. Consulte "Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager Connector," página 10.
- Compruebe que dispone de al menos 2 GB de espacio en el disco en la partición raíz primaria del dispositivo.
- Compruebe que el conector está configurado correctamente.
- Realice una snapshot del dispositivo conector como copia de seguridad. Para obtener información sobre cómo realizar snapshots, consulte la documentación de vSphere.
- Si para el acceso HTTP saliente se necesita un servidor proxy HTTP, configure los valores del servidor proxy para el dispositivo conector. Consulte "Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager Connector," página 10.

Requisitos previos para la actualización sin conexión

- Confirme que existe una actualización del conector. Compruebe si hay actualizaciones en el sitio de descargas de My VMware en my.vmware.com.
- Compruebe que dispone de al menos 2 GB de espacio en el disco en la partición raíz primaria del dispositivo.

- Compruebe que el conector está configurado correctamente.
- Realice una snapshot del dispositivo conector como copia de seguridad. Para obtener información sobre cómo realizar snapshots, consulte la documentación de vSphere.
- Configure el dispositivo conector para usar un servidor web local para alojar el archivo de actualización. Consulte Capítulo 4, "Realizar una actualización de VMware Identity Manager Connector sin conexión.," página 15.

Comprobar la disponibilidad de una actualización en línea de VMware Identity Manager Connector

Si su dispositivo conector tiene conexión a Internet, puede comprobar la disponibilidad de actualizaciones en línea desde el dispositivo.

Procedimiento

1 Inicie sesión en el dispositivo conector como usuario raíz.

2 Ejecute el comando siguiente.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.

```
/usr/local/horizon/update/updatemgr.hzn check
```

Configurar las opciones del servidor proxy para el dispositivo de VMware Identity Manager Connector

El dispositivo conector accede a los servidores de actualización de VMware a través de Internet. Si su configuración de red proporciona acceso a Internet con un proxy HTTP, debe modificar la configuración del dispositivo.

Habilite su proxy para gestionar solo el tráfico de Internet. Para garantizar que el proxy se configura correctamente, establezca el parámetro del tráfico interno en la opción sin proxy en el dominio.

NOTA: Los servidores proxy que requieren autenticación no son compatibles.

Prerequisitos

- Compruebe que dispone de la contraseña raíz del dispositivo conector.
- Compruebe que dispone de la información del servidor proxy.

Procedimiento

1 Inicie sesión en el dispositivo conector como usuario raíz.

2 Introduzca `YaST` en la línea de comandos para ejecutar la utilidad `YaST`.

3 En el panel izquierdo, seleccione **Servicios de red** y, a continuación, **Proxy**.

4 Introduzca las URL del servidor proxy en los campos de **URL del proxy HTTP** y **URL del proxy HTTPS**.

5 Seleccione **Finalizar** y salga de la utilidad `YaST`.

6 Reinicie el servidor Tomcat en el dispositivo virtual conector para utilizar la nueva configuración del proxy.

```
service horizon-workspace restart
```

Los servidores de actualización de VMware ya están disponibles para el dispositivo conector.

Realizar una actualización en línea de VMware Identity Manager Connector

3

Puede actualizar su instancia de VMware Identity Manager Connector en línea.

Prerequisitos

- Se deben cumplir los requisitos previos indicados en Capítulo 2, "Preparar la actualización de VMware Identity Manager Connector," página 9.
- Compruebe que el dispositivo conector esté encendido y en funcionamiento.

Procedimiento

1 Inicie sesión en el dispositivo conector como usuario raíz.

2 Ejecute el comando siguiente.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 Ejecute el comando siguiente para comprobar si existe una actualización en línea.

```
/usr/local/horizon/update/updatemgr.hzn check
```

4 Ejecute el comando siguiente para actualizar el dispositivo.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.

5 Vuelva a ejecutar el comando `updatemgr.hzn check` para comprobar que no existe ninguna actualización más reciente.

```
/usr/local/horizon/update/updatemgr.hzn check
```

6 Compruebe la versión del dispositivo actualizado.

```
vamicli version --appliance
```

Se mostrará la nueva versión.

7 Reinicie el dispositivo conector.

```
reboot
```

8 Repita los pasos anteriores en cada dispositivo conector en su implementación de VMware Identity Manager.

Se completó la actualización del conector.

Realizar una actualización de VMware Identity Manager Connector sin conexión.

4

Si el dispositivo VMware Identity Manager Connector no se puede conectar a Internet para su actualización, se puede realizar una actualización sin conexión. Se debe configurar un directorio de actualización en un servidor web local y configurar el dispositivo conector para utilizarlo para la actualización.

Este capítulo cubre los siguientes temas:

- "Preparar un servidor web local para la actualización sin conexión," página 15
- "Configurar el conector y realizar una actualización sin conexión," página 16

Preparar un servidor web local para la actualización sin conexión

Antes de iniciar la actualización del conector sin conexión, se debe preparar el servidor web local creando una estructura de directorios que incluya un subdirectorio para el dispositivo conector.

Prerequisitos

- Descargue el archivo `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` desde My VMware. Acceda a my.vmware.com, diríjase a la página de descargas de VMware Identity Manager y descargue el archivo que aparece en la lista de la sección **Paquete de actualización sin conexión del conector de VMware Identity Manager**.
- Si utiliza un servidor web IIS, configúrelo para que admita caracteres especiales en los nombres de archivo. Para ello, acceda a la sección **Filtrado de solicitudes** y seleccione la opción **Permitir doble escape**.

Procedimiento

1 Cree un directorio en el servidor web en http://*SuServidorWeb*/*VM*/ y copie en él el archivo descargado.

2 Verifique que el servidor web incluya los tipos mime para `.sig` (texto/simple) y `.sha256` (texto/simple).

Si estos tipos de mime, el servidor no podrá comprobar si hay actualizaciones.

3 Descomprima el archivo.

El contenido extraído del archivo ZIP será proporcionado por http://*SuServidorWeb*/*VM*/.

El contenido extraído del archivo contiene los siguientes subdirectorios `/manifest` y `/package-pool`.

4 Ejecute el comando siguiente `updatelocal.hzn` para comprobar que en la URL hay contenido de actualización válido.

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM
```

Configurar el conector y realizar una actualización sin conexión

Configure el dispositivo conector para indicarle al servidor web local que realice una actualización sin conexión. A continuación, actualice el dispositivo.

Prerequisitos

"Preparar un servidor web local para la actualización sin conexión," página 15.

Procedimiento

1 Inicie sesión en el dispositivo conector como usuario raíz.

2 Ejecute el siguiente comando para configurar un repositorio de actualización que utilice un servidor web local.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://YourWebServer/VM/
```

NOTA: Para deshacer los cambios de la configuración y restablecer la opción de realizar una actualización en línea, puede ejecutar el siguiente comando.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

---

3 Realice la actualización.

a Ejecute el comando siguiente.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

b Ejecute el comando siguiente para comprobar la versión de la actualización disponible.

```
/usr/local/horizon/update/updatemgr.hzn check
```

c Ejecute el comando siguiente para actualizar el conector.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Los mensajes que se generen durante la actualización se guardan en el archivo `update.log` en `/opt/vmware/var/log/update.log`.

d Vuelva a ejecutar el comando `updatemgr.hzn check`.

```
/usr/local/horizon/update/updatemgr.hzn check
```

e Compruebe la versión del dispositivo actualizado.

```
vamicli version --appliance
```

El comando debe mostrar la nueva versión.

f Reinicie el dispositivo conector.

Por ejemplo, desde la línea del comando, ejecute el siguiente comando.

```
reboot
```

4 Repita los pasos anteriores en cada dispositivo conector en su implementación de VMware Identity Manager.

Se completó la actualización del conector.

Realizar la configuración después de actualizar el conector

5

Después de actualizar al conector 2016.3.1.0 o posterior, configure las siguientes opciones.

- Si utiliza directorios de Active Directory (Autenticación de Windows integrada), ThinApps o la autenticación de Kerberos, debe salir del dominio y, a continuación, volver a entrar. Este paso es obligatorio para todos los dispositivos virtuales conectores de su implementación.
  a Haga clic en la pestaña **Administración de acceso e identidad**.
  b Haga clic en **Configurar**.
  c En la página Conectores, haga clic en **Dejar el dominio** en cada conector que se está utilizando en el directorio de Active Directory (Autenticación de Windows integrada), la integración de ThinApps o la autenticación de Kerberos.
  d Haga clic en **Unirse al dominio** para volver a entrar en el dominio.

    Para unirse al dominio, necesita las credenciales de Active Directory con los privilegios para unirse. Consulte "Integrar con Active Directory" en *Instalar y configurar VMware Identity Manager* para obtener más información sobre cómo unirse a un dominio.
  e Si utiliza la autenticación de Kerberos, vuelva a habilitar el adaptador de esta autenticación. Para acceder a la página Adaptadores de autenticación, haga clic en el vínculo adecuado en la columna **Trabajo** y seleccione la pestaña **Adaptadores de autenticación** en la página Conectores.
  f Compruebe que el resto de adaptadores de autenticación que está utilizando están habilitados.
- Si utiliza Active Directory (Autenticación de Windows integrada) o Active Directory mediante LDAP con la opción **Este directorio admite la ubicación de servicio de DNS** habilitada, guarde la página de los dominios del directorio.
  a Haga clic en la pestaña **Administración de acceso e identidad**.
  b En la página Directorios, haga clic en el directorio.
  c Proporcione la contraseña del usuario de DN de enlace y haga clic en **Guardar**.
  d Haga clic en **Configuración de sincronización** en la parte izquierda de la página y seleccione la pestaña **Dominios**.

e Haga clic en **Guardar**.

NOTA: En la versión 2016.3.1.0 o versiones posteriores del conector, se crea automáticamente un archivo `domain_krb.properties` que se rellena de forma automática con controladores de dominio cuando se crea un directorio con la ubicación del servicio DNS habilitada. Cuando guarda la página Dominios tras realizar la actualización, si disponía de un archivo `domain_krb.properties` en su implementación original, el archivo se actualiza con los dominios que pudo agregar posteriormente y que no se encontraban en el archivo. Si no disponía de un archivo `domain_krb.properties` en su implementación original, se creará y rellenará de forma automática con controladores de dominio. Consulte "Integrar con Active Direcetory" en *Instalar y configurar VMware Identity Manager* para obtener más información sobre el archivo `domain_krb.properties`.

Resolver problemas de actualización 6

Para resolver problemas de actualización, revise los archivos de registro. Si el conector no se inicia después de la actualización, se puede restaurar una instancia anterior a partir de una snapshot.

Este capítulo cubre los siguientes temas:

- "Consultar los registros de errores de la actualización," página 19
- "Restaurar snapshots del conector," página 19
- "Recopilar un paquete de archivos de registro," página 20

Consultar los registros de errores de la actualización

Revise los registros de errores ocurridos durante la actualización para resolverlos. Los archivos de registro de la actualización están en el directorio `/opt/vmware/var/log`.

Problema

Al finalizar la actualización, el conector no se inicia y los errores aparecen en los registros de errores.

Origen

Errores ocurridos durante la actualización.

Solución

1 Inicie sesión en el dispositivo del conector.

2 Acceda al directorio `/opt/vmware/var/log`.

3 Abra el archivo `update.log` y revise los mensajes de error.

4 Resuelva los errores y vuelva a ejecutar el comando de actualización. El comando de actualización continuará desde el punto en que se detuvo.

NOTA: También puede revertir a una snapshot y ejecutar de nuevo la actualización.

Restaurar snapshots del conector

Si el conector no se inicia correctamente después de una actualización, se puede restaurar una instancia anterior.

Problema

Después de actualizar la instancia del conector, sigue sin iniciarse correctamente. Se revisaron los registros de errores de actualización y se ejecutó de nuevo el comando de actualización, pero no se resolvió el problema.

Origen

Ocurrieron errores durante el proceso de actualización.

Solución

- Realice la restauración utilizando una de las snapshots realizadas como copia de seguridad de la instancia original del conector. Para obtener información, consulte la documentación de vSphere.

Recopilar un paquete de archivos de registro

Puede recopilar un paquete de archivos de registro para enviárselo al equipo de soporte técnico de VMware. El paquete se obtiene de la página de configuración del conector.

El paquete incluye los siguientes archivos de registro.

Tabla 6-1. Archivos de registro

Componente	Ubicación del archivo de registro	Descripción
Registros de Apache Tomcat (catalina.log)	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat registra los mensajes que no se registran en otros archivos de registro.
Registros del configurador (configurator.log)	`/opt/vmware/horizon/workspace/logs/configurator.log`	Solicitudes que recibe el configurador del cliente REST y de la interfaz web.
Registros del conector (connector.log)	`/opt/vmware/horizon/workspace/logs/connector.log`	Un registro de cada solicitud recibida desde la interfaz web. Cada entrada del registro incluye también la URL, la marca de hora y las excepciones de la solicitud. No se registra ninguna acción de sincronización.

Procedimiento

1 Inicie la sesión en la página de configuración del conector en https://*connectorURL*:8443/cfg/logs.

2 Haga clic en **Preparar paquete de registro**.

3 Descargue el paquete y envíelo al equipo de soporte técnico de VMware.

Índice

A

actualizar **7, 13, 15**
archivo domain_krb.properties **17**
archivos de registro **20**

C

catalina.log **20**
comprobar **10**
configurar **10, 16**
configurator.log **20**
connector.log **20**

E

errores posteriores a la instalación **19**

G

glosario **5**

P

paquete de registro **20**
preparar **9, 15**
proxy HTTP **10**
público objetivo **5**

R

registro de errores **19**
requisitos previos de actualización **9**
restaurar **19**

S

servidor proxy **10**
servidor web local **15, 16**
snapshot **19**
solucionar problemas **19**

U

unirse a un dominio **17**
update.log **19**